1/9/1 **Links**
Fulltext available through: USPTO Full Text Retrieval Options
ABI/Inform(R)

01579770 02-30759

Today's window of exposure for data loss

Buffington, Jason L
Computer Technology Review Storage Inc. Supplement pp: 74-81
Winter 1997
ISSN: 0278-9647 **Journal Code:** CTN
Document Type: Journal article **Language:** English **Length:** 6 Pages
Special Feature: Graphs
Word Count: 3189

Abstract:

Proper capacity planning for an automated tape library, along with proper understanding of the nature of one's data and ensuring stability of the tape backup software, can yield a successful archival solution. However, that is really all it yields - an archival solution. There are four main reasons why a backup window is necessary: open files, CPU utilization, network utilization, and server stability. The problem with the backup window is that it is inevitably too small. The window of exposure is defined as the amount of time between data protection efforts; or more simply, the maximum amount of time over which data could be lost. For tape backup systems, the best case window of exposure is twenty-three hours and fifty-nine minutes, i.e., from the moment the backup finishes a file and until it touches it again. There is hope for legitimately reducing one's window of exposure - with a different approach to file system replication.

Text:

Last week, while on site in Houston, I was notified by my client that the server that we were in the process of auditing had no downtime. That did not mean that the server never failed. It meant that no one was EVER allowed to bring the server down-not for scheduled maintenance or patches, not for recycling of the memory pool (this was NetWare 3.12), not for anything.

This server was the single point of gas trading for a large energy company in Houston and gas is traded literally twenty-four hours per day and seven days per week. Consequently, if anything new had to be loaded on the server, the NLMs were installed and added to the startup files and when the server next abended and came back up, the modules would be loaded. As long as the new software had been properly tested, this method was risky but seemed to work for them. My main concern with this approach is that if the

server had recently abended and then had problems with new software on its way back up; chances were pretty good that it would be abending again, and soon. But, that was the customer's decision-"no downtime". You may or may not have that same level of criticality in your server(s), but the desired condition is the sameno downtime.
(Photograph Omitted)

Taking a step back from that goal, a more attainable objective is actually no loss of data. It used to be that a reliable and automated tape backup system could solve this objective. While many people may say that "reliable" and "tape backup system" are a contradiction in terms, tape backup problems really can be solved. Proper capacity planning for an automated tape library, along with proper understanding of the nature of one's data and ensuring stability of the tape backup software, can yield a successful archival solution. And that is really all it yieldsan archival solution. Two adages that everyone knows, but no one says are, "You're only as protected as your last backup" and "No one wants backup, but everyone needs restore". Together these two truisms spell out the limitations of any backup solution. If your backup ran last night at midnight and the most important file on your server was written to tape at 1:45 in the morning, then for the next 23 hours, any changes made to that file will probably be lost. This is assuming that you are able to back up that file every day. This leads us to my first tangent topic-the backup window.

There are four main reasons why a backup window is "necessary": open files, CPU utilization, network utilization, and server stability. Whether the server supports file access, e-mail, or a client/server application, it is guaranteed that all files in use will be in a locked state. This means that the backup application cannot secure the file to be written to tape because user(s) or application engines have the file locked exclusively = open files. There are agent technologies that will circumvent this problem for a particular type of file or application, but these are relatively expensive and usually cumbersome. The second common issue that necessitates a backup window is CPU utilization. During the backup of a server, its CPU will skyrocket. And if this happened in the middle of the business day, everything else on the server will slow down! Similarly, unless you have a backup application and hardware on every server, data being backed up will have to travel the network to the "backup server"-again slowing down the user community. And finally, regardless of what backup application that you run, sooner or later your software will abend the server. This is not always (but sometimes) due to errors in the software, but just the nature of backup. Almost everyone has heard the radio commercials regarding, "the worst thing you can do to your car is starting and stopping." Well, the harshest thing to do to a server is back it up. Nothing will tax the network card, disk channel, I/O bus, processor and memory more than backing up the data. And, sooner or later, it will break (i.e. abend, blue-screen, hexdump, etc.). To minimize all of these problems, network administrators are forced to run their backups from late in the evening until early in the morning. This reduces the number of open files, minimizes the impact of high CPU utilization and low network bandwidth, and lessens the impact of an abending server-i.e. "the backup window".

The problem with the backup window is that it is inevitably too small. The national or global nature of Corporate America, along with the growing number of laptop users, is stretching the business day; thus, reducing the window of opportunity. In addition, applications and data areas are growing larger-requiring more and more backup time, while the backup window is ever smaller. Regardless of what your particular backup window allows you to back-up, during every other point of the day, that data is unprotected. If the CFO began a document at 10a.m., worked on it until 4p.m., and then accidentally erased it, it's gone! That file was never secured to tape and is therefore unrecoverable. The file was created, edited and deleted outside of the backup window-or by this article's definition, within "the window of exposure".

The window of exposure is defined as the amount of time between data protection efforts; or more simply, the maximum amount of time over which data could be lost. For tape backup systems, the best case window of exposure is twenty-three hours and fiftynine minutes-i.e. from the moment the backup finishes a file and until it touches it again. In most Grandfather/Father/ Son rotation systems, the window of exposure might actually be a full week.

Continuing on with the perspective of the window of exposure, it is appropriate to consider "server clusters" and/or "application clusters". Server clusters are not a relatively new concept, just new to NetWare and Windows NT environments (i.e. Wolf Mountain and Wolf Pack, respectively). Application clusters for Oracle, Lotus Notes, etc. are also not atypical. Both provide a level of high availability, but from an operational perspective, they are almost exact opposites. The initial offerings in server clusters are two processing nodes that share a single storage array. This gives both "halves" equal access to the disk areas and if one node were to go down, the other would continue to service the requests. Application clustering is usually implemented by running the same application on multiple servers with the application being responsible for synchronizing the data throughout all of the various locations. Then, if a client's server goes down, they can simply connect to another copy of the data. Unfortunately, neither of these architectures protects from data loss, only resource outage. If the server cluster's one copy of the data, or the application cluster's instance of the data, becomes corrupted or otherwise lost, there is no recovery. One must go back to whatever tape solution is in place. Interestingly, file areas that are typically placed on server or application clusters are usually put there because of their high availability requirement. This also implies that the files will be in use most, if not all, of the time. Thus, we are back to the problem of a nonexistent backup window-or a large window of exposure for data loss (See Fig).

Most network administrators' only attempt at data protection (other than tape backup) is fault tolerant storage systems. With this in mind, no article on data protection would be complete without discussing RAID. For clarification, when people refer to RAID (Redundant Array of Inexpensive Disks), they are typically referring to RAID level Five. RAIDS specifies how for any number of disks, a "stripe" of data is written across them with N minus 1 of the blocks containing data and the other containing "parity". This allows the contents of any block in the stripe to be recalculated, based on the contents of the rest of the stripe. Furthermore, the parity blocks are distributed between all of the drives, such that no single drive is a point of failure. The benefit is that if a drive fails, the RAID set can continue to function. One does lose the capacity of a whole drive, meaning that if five 4GB drives are RAID'ed together, the capacity of the RAID array is 16GB, and not 20GB.

There is also a performance advantage to RAIDS, in that disk reads are spanned over all N drives, so instead of waiting for a single drive to read four blocks of data, the RAID set can produce the data in almost 1/Nth of the time.

(Graph Omitted)

Captioned as: Fig The window of exposure refers to the maximum amount of time over which data can be lost.

There are few arguments in life, or at least in one's Techno-professional-life, that are fought as hard as the debate of RAI5S versus Mirroring (or duplexing). For clarification, mirroring refers to two disks on the same disk controller that are always synchronized. If either drive fails, the other continues without mishap. Mirroring also has a performance advantage, in that disk reads are read from the first available disk-virtually doubling performance. Mirroring has the disadvantage of losing half of the total drive capacity; meaning that if eight drives are mirrored, the total storage capacity is four drives. Duplexing builds on mirroring, with one advantage-the drives are on separate controllers. This guarantees the availability of a drive set, in case either disk controller fails. The "controller failure" liability exists for both mirroring and RAID, but not duplexing. It is important to note that the possibility of controller failure is not as remote as one might imagine. If a tape drive,or CD-ROM drive were to lock up and not "release" the SCSI channel, the whole channel (including all disks and the controller) would be unavailable. For the sake of the RAIDS versus Duplexing argument, I prefer duplexing. Yes, it costs more. For the capacity of four drives, one must buy five for RAID5 (typically six for a hot spare) or eight for a duplexed solution. If you lose one drive in either configuration, the server continues. If you lose two drives, the RAID solution will fail. The duplexing solution will only fail if the second failed drive was the twin of the first, and then only for that logical drive-not the rest of the data set. My opinion is that disks are relatively cheap and once you've stepped from four to six, eight doesn't seem that much higher for the added protection. One positive side note- almost all of the higher-end disk control-lers that provide hardware-based RAIDS can support mirroring/ duplexing, as well.

In regard to the "Window of Exposure" for Data Loss, none of this matters. That may be a strong statement to make until you consider that in 1996, seven out of eight (88%) of all server failures were software based. That means that all of the redundant disks, controllers, power supplies, etc. addressed twelve percent of the problem! And in most of those cases, when the server was restored, the data was intact.

A wise man once said, "Never complain about a problem, unless you have an idea how to solve it." I'm not sure if this is entirely true, but it works to transition me into talking about the various solutions that are available, today. There are three basic techniques in reducing the window of exposure for data loss: mirroring extensions, application replication, and file system replication. The first two are really approaches to high availability but are sometimes applied to data protection.

"Mirroring Extensions" refers to allowing a production server to mirror two sets of disks; but, in actuality, one of the disk sets is physically connected to a redundant server. If the primary server were to fail, the second server would reboot and take over by mounting the mirrored drives from the production server. This is similar to the server clustering principles that we discussed earlier. Two server nodes share one logical file system. In clustering, they shared one physical drive array. In extensions, there are two drive arrays, but one logical representation, since they are mirrored. This leads to the same problem, if the only copy of the data becomes corrupt or deleted, we are back to whatever was provided by a tape backup solution. One tangent approach to extensions of mirroring is to temporarily halt the mirroring process. During this time, the second server's drives are dormant and can be backed up. However, during this time, the high availability protection is hindered because if the production server fails, the second copy is no longer current! The proposed advantage of this model is that the second file system is frozen, so backups of typically open files (databases, e-mail systems, etc.) are able to be secured to tape without agent technologies. As we've stated previously, however, a tape backup is only as good as it is current, so to reduce our window of exposure, one would have to "halt the mirroring, perform a backup, restart the mirroring and synchronize"-as many times per day as feasible. Another tangent approach is create shadow images or freeze frames of the second drives' file system for the purpose of backing it up, while the data changes continue to be updated. However, if the server is significantly active, the frozen images of the files that have changed during the backup can overwhelm the memory and/or disk reserves on the redundant server; thus, precluding practical use during the business day.

There are two definitions for "Application Replication". The first refers

to the synchronization of data between client server engines. We have already discussed this model (see clustering section above). The other definition that is also known as "file replication" refers to a different methodology of high availability-the idea of monitoring application files for changes. If a production server marks a file as changed (e.g. archive bit or time stamp), then some process copies the file to a second server. This has the high availability potential of being able to stand in for the failed production server and the backup possibility of providing for backing up the second copy of the data, at will. In fact, some variations of this technology merge the two concepts by storing the second data set exclusively on tape, instead of disk. This alternative offers two benefits, one guarantees that backups are conducted (by eliminating the need for separate backup software) and also reducing the amount of disk required to store the files. While the latter benefit is legitimate, the former has one major fallacy. The companies that offer this solution are not Cheyenne, or Seagate, or Legato, or anyone else that has been developing backup technologies for over two years. It is sufficient to say, that they may not be the best technology to whom I would want to trust my "backups" to. Strike number two comes from the fact that the benefit of storing directly to tape becomes a burden if in fact one wishes to utilize the high availability capability. Then, the users will actually be trying to pull their applications from tape (too slow) or wait while the data is regurgitated from tape to disk, as fast as possible. The third strike for this methodology is that a copy of the production file will be sent every time a change is detected. If the file is multi-user file (e.g. a database), then every time any user updates any single cell, a copy of the whole file will be sent to the second server! Theoretically, the file could literally be streamed back to back with itself, over and over again, even though 99% of the contents are the same between each two versions. As an added detriment, the sending operation is simply a "file read" operation to the server OS, which results in a significant amount of added I/O load to the server.

The newest approach to reducing the window of exposure for data loss is "file system replication". Again, there are two accepted implementations of this term: one is the replication of files and directories to multiple servers and the other being the future "distributed" file system. In consideration of the distributed file system, first, one can only speculate, since neither Novell or Microsoft has actually released an offering. Both offerings promise to "blur the lines between servers" much the same way that the difference between files stored on one's PC and on the server is blurred to the user community today. Based on that description, one can speculate that while data may be more spread out, there will be only one logical representation of that file throughout the enterprise. And following in the logical evolution of mirroring-extensions and clustering, it is fair to assume that the same limitation will apply-if that one copy of the file is corrupted or lost, we must look back to tape. Similar to the clustered approach, a distributed file system will provide for access to the file over longer distances, thus reducing the backup window and increasing the window of exposure.

However, there is hope for legitimately reducing one's window of exposurewith a different approach to file system replication. With more recent technology and product offerings, the shift is being made to identifying key directories and files, or entire file systems, and replicating the logical changes within the files to a second server. Thus, even in a multi-gigabyte database, if one cell's contents were changed (e.g. 5KB), only those 5KB would be transmitted to the second server. By transmitting on the "writes" and not the "reads" and at such a granular level, "real-time" is achievable and network bandwidth is hardly a concern; regardless of the amount of actual storage. These approaches provide for the benefits of recurring backup during the day; by providing a second copy of the data to be dormant, but up to date, continuously. This virtually expands the backup window to twenty-four hours; thereby, eliminating the window of exposure almost completely! These technologies are able to secure those changes in the data within the OS kernel (without having to re-read the entire file), which significantly reduces the overhead on the production server(s); and these transactions are secured and replicated in "real-time". It is important to note that for "file systems" to be accurately replicated, it is necessary to replicate the security model, as well. This implies retaining, and possibly translating, trustee assignments and file attributes between the various copies of the file - in sync with the data changes within the file.

It is evident that this functionality will be necessary in tomorrow's network operating systems to truly support the clustered and distributed topologies of the next generation; but today only two companies offer this functionality. NSI Software offers Double-Take for Windows NT, NetWare, and UNIX and can be reached at 800-775-4674 (www.nsisw.com). And Qualix (formerly known as Octopus) offers similar functionality for Windows NT and Windows 95, and can be reached at 800245-8649 (www.qualix.com).

Author Affiliation:

Jason Buffington is a systems engineer at NSI Software (Hoboken, NJ).

Author Affiliation:

www.nsisw.com

THIS IS THE FULL-TEXT.

Geographic Names: US

Descriptors: Back up systems; Tape operating systems ; Servers
Classification Codes: 9190 (CN=United States); 5240 (CN=Software & systems)

[File 347] **JAPIO** Dec 1976-2005/Dec(Updated 060404)

[File 350] **Derwent WPIX** 1963-2006/UD,UM &UP=200643

**File 350: Preview the enhanced DWPI through ONTAP DWPI (File 280). For more information, visit http://www.dialog.com/dwpi/.*

```
 ; d s
Set     Items   Description
S1     200577   S SERVER? OR RAS OR KEYSERVER? OR MAILSERVER? OR MULTISERVER? OR
WEBSERVER? OR PRINTSERVER? OR FILESERVER? OR HTTPSERVER? OR FTPSERVER?
S2         24   S CLIENTSERVER? OR MICROSERVER? OR MINISERVER? OR PROXYSERVER? OR
DATASERVER?
S3          1   S MAINSERVER? OR CENTRALSERVER? OR HEADSERVER? OR HOSTSERVER? OR
LEADSERVER? OR HEADSERVER? OR MASTERSERVER? OR CHIEFSERVER?
S4          0   S ALPHASERVER? OR HUBSERVER?
S5       9824   S (MAIN OR CENTRAL OR HEAD OR HOST OR LEAD OR MASTER OR CHIEF OR ALPHA OR
HUB OR CONTROL OR PRIMARY OR CENTER OR PARENT)(1W)S1:S2
S6         80   S (ADMINSTRAT???? ? OR PRINCIPAL OR PRINCIPLE OR LEADER OR CHIEF OR PRIME
OR ALPHA OR ARCHIV??? ? OR FOREMOST)(1W)S1:S2
S7        126   S (HEADMOST OR ORIGINAL OR HUB)(1W)S1:S2
S8          2   S SUPERIOR(1W)S1:S2
S9          0   S MAJOR(1W)S1:S2
S10      1346   S (SECONDARY OR LOCAL OR NODE OR CHILD OR SLAVE? OR BETA OR DEPENDENT OR
SUBORDINAT? OR INFERIOR OR MINOR OR SUBSERVIEN?)(1W)S1:S2
S11        85   S LOCALSERVER? OR NODESERVER? OR CHILDSERVER? OR SLAVESERVER? OR
SUBSERVER? OR BETASERVER? OR MINORSERVER? OR SUB()SERVER?
S12    146059   S DB OR DBS OR DATABASE? OR DATASET? OR DATABANK? OR DATASTORE? OR
DATAFILE? OR DATASYSTEM? OR DATALIBRAR? OR DATAMART?
S13    177287   S DATA()(BASE? ? OR SET? ? OR BANK? ? OR STORE? ? OR FILE? ? OR SYSTEM? ?
OR LIBRAR??? ? OR MART? ? OR COLLECTION? OR DEPOSIT? OR REPOSIT?)
S14       588   S DATA()(WAREHOUS? OR STOREHOUS? OR (WARE OR STORE)()HOUS???? ?)
S15      1859   S DBMS? OR RDB? ? OR VLDB? ? OR LDB? ? OR ODBC? ? OR OODB? ? OR RDBM? ? OR
OODM? ? OR ODBM? ?
S16    142218   S FILE OR FILES
S17         1   S COMPUTERFILE? OR TEXTFILE?
S18      1679   S S12:S17(3N)(FREEZ? OR FROZE? OR LOCK??? ? OR LATCH? OR FLIPFLOP? OR
FLIP()FLOP? OR SUSPEND? OR SUSPENS? OR CEAS???? ? OR CESSATION?)
S19       588   S S12:S17(3N)(INTERRUPT? OR ARREST? OR PAUS??? ? OR ABEYAN?)
S20        30   S S12:S17(3N)TEMPORAR?(1W)(HALT??? ? OR STOP???? ? OR HOLD OR HELD OR
STAY??? ? OR DISCONTINU? OR INHIBIT?)
S21        66   S S12:S17(3N)TEMPORAR?(1N)(HALT??? ? OR STOP???? ? OR HOLD OR HELD OR
STAY??? ? OR DISCONTINU? OR INHIBIT?)
S22     10325   S S12:S17(3N)(REPLICA? OR DUPLICAT? OR COPIE? ? OR COPY??? ? OR MIRROR? OR
REPRODUC????? ? OR SHADOW? OR BACKUP? OR BACK??? ?()UP? ?)
S23      1241   S S12:S17(3N)(CLONE? ? OR CLON??? ? OR FACSIMILE? OR RE()PRODUC????? ?)
S24       126   S S18:S21 AND S22:S23
S25         3   S S24 AND S10:S11
S26         0   S S24 AND CLIENTSERVER?
S27         7   S S24 AND S3:S9
S28         7   S S25 OR S27
 ; t 28/9/2,4,6-7
```

28/9/2 (Item 1 from file: 350) **Links**
Derwent WPIX

017408625 **Image available**
WPI Acc No: 2005-732288/200575
XRPX Acc No: N05-602773

Database access enabling system for use in network, has suspending unit momentarily suspending primary database unit for keeping consistency between two databases, and mirroring system mirroring backup database

Patent Assignee: UNISYS CORP (BURS)
Inventor: HART D R; LIN S E
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6957221	B1	20051018	US 2002235763	A	20020905	200575	B

Priority Applications (No Type Date): US 2002235763 A 20020905
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6957221	B1		16	G06F-017/30	

Abstract (Basic): US 6957221 B1

NOVELTY - The system has a data consistency maintaining unit to maintain physical data consistency between a primary **backup** database and a secondary **backup database** (25). A **suspending** unit momentarily **suspends** the primary **database** unit for keeping consistency between **databases**. A **mirroring** system (26) **mirrors** the **backup database** (25), and a utilizing unit utilizes the mirrored disk **copy** as a **backup database.**

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(A) an online transaction system for enabling continuous database operations in a network comprising audit files transmitting unit

(B) a method for enabling continuous updating in **primary server** unit

(C) a method for capturing a snapshot of data from an on-line transaction processing system

(D) a network utilizing a primary database system.

USE - Used for enabling database access to a client-user in a primary database unit in a network (claimed).

ADVANTAGE - The mirroring system **mirrors** the secondary **backup database** to be utilized as the **backup database** for informational access, without distributing the secondary database and ongoing operations, thus improving database availability for updated information, and enhancing performance of the enabling system.

DESCRIPTION OF DRAWING(S) - The drawing shows a system depicting a **primary-host server, secondary host server**, and a disk subsystem supporting the servers.

Servers (10, 18)

Database system (14, 22)
Disk volume (23)
Secondary **backup database** (25)
Mirroring system (26)
pp; 16 DwgNo 2/6

Title Terms: DATABASE; ACCESS; ENABLE; SYSTEM; NETWORK; SUSPENSION; UNIT; MOMENTARY; SUSPENSION; PRIMARY; DATABASE; UNIT; KEEP; CONSISTENCY; TWO; MIRROR; SYSTEM; MIRROR; DATABASE
Derwent Class: T01
International Patent Class (Main): G06F-017/30
File Segment: EPI
Manual Codes (EPI/S-X): T01-F02C1; T01-F05E; T01-G03; T01-H01C3; T01-J05B4M ; T01-N02A3C; T01-S02

28/9/4 (Item 3 from file: 350) **Links**
Derwent WPIX

016221065 **Image available**
WPI Acc No: 2004-378953/200436
XRPX Acc No: N04-301567

Database system has local servers that freeze local databases and cause local storage sub-system to replicate local databases in center storage sub-system, on receiving database replication request from center server

Patent Assignee: HITACHI LTD (HITA); EGUCHI Y (EGUC-I); IDEI H (IDEI-I); MOGI K (MOGI-I); NISHIKAWA N (NISH-I)
Inventor: EGUCHI Y; IDEI H; MOGI K; NISHIKAWA N
Number of Countries: 033 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1420350	A2	20040519	EP 200318158	A	20030808	200436	B
US 20040098417	A1	20040520	US 2003634993	A	20030806	200436	
JP 2004164401	A	20040610	JP 2002330731	A	20021114	200438	

Priority Applications (No Type Date): JP 2002330731 A 20021114
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1420350	A2	E	14	G06F-017/30	

Designated States (Regional): AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20040098417	A1			G06F-012/00	
JP 2004164401	A		14	G06F-012/00	

Abstract (Basic): EP 1420350 A2

NOVELTY - A **center server** requests **local servers** to **replicate** local **databases** (**DBs**), and consolidates the **replicated** local **DBs**. The **local servers** request the **database** management systems to **freeze** the local **DBs**, and cause a local storage sub-system to **replicate** the stored **DBs** in a center storage sub-system, on receiving the **database replication** request.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(1) **center server**;

(2) database system access method;

(3) program for executing a process in **center server**; and

(4) program for executing a process in **local server**.

USE - For instantaneous access of databases at remote locations through local area network (LAN).

ADVANTAGE - Consolidated access to the databases at the remote locations is ensured instantaneously.

DESCRIPTION OF DRAWING(S) - The figure shows a block diagram of the database system.

pp; 14 DwgNo 1/6

Title Terms: DATABASE; SYSTEM; LOCAL; SERVE; FREEZE; LOCAL; CAUSE; LOCAL; STORAGE; SUB; SYSTEM; REPLICA; LOCAL; STORAGE; SUB; SYSTEM; RECEIVE; DATABASE; REPLICA; REQUEST; SERVE

Derwent Class: T01

International Patent Class (Main): G06F-012/00; G06F-017/30

File Segment: EPI

Manual Codes (EPI/S-X): T01-J05B4A; T01-J05B4P; T01-S03

28/9/6 (Item 5 from file: 350) Links

Derwent WPIX

012210411 **Image available**

WPI Acc No: 1999-016517/199902

XRPX Acc No: N99-013280

Video program transmitting method - involves copying video program of main server onto cache server after modification of playback file contents, when interrupted during original copying

Patent Assignee: SONY CORP (SONY)

Inventor: NORITOMI M

Number of Countries: 002 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 10285510	A	19981023	JP 9787075	A	19970404	199902	B
US 6473902	B1	20021029	US 9853772	A	19980402	200274	

Priority Applications (No Type Date): JP 9787075 A 19970404

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 10285510	A		25	H04N-005/765	
US 6473902	B1			H04N-007/173	

Abstract (Basic): JP 10285510 A

The method involves copying a video program currently stored by a **main server** (4) onto a cache server (5). A database file consists of information on video program currently stored by cache server. A playback file (121) consists of information on transmitting program of cache server. A **copy file** (123) specifies video program stored in the playback file but not in a database (122).

A copy demand is sent to the **main server**, based on which the currently stored video program is copied to the cache. When there is modification of video program in the playback **file**, **copying** is **interrupted** and a copy demand is sent after modification, based on which data are copied to cache server.

ADVANTAGE - Improves copying efficiency. Performs interrupted copying, reliably.

Dwg.1/26

Title Terms: VIDEO; PROGRAM; TRANSMIT; METHOD; COPY; VIDEO; PROGRAM; MAIN; SERVE; CACHE; SERVE; AFTER; MODIFIED; PLAYBACK; FILE; CONTENT; INTERRUPT; ORIGINAL; COPY
Derwent Class: W02; W04
International Patent Class (Main): H04N-005/765; H04N-007/173
International Patent Class (Additional): G06F-009/00; G06F-015/16; H04N-005/781; H04N-007/16
File Segment: EPI
Manual Codes (EPI/S-X): W02-F05A; W04-B; W04-K

28/9/7 (Item 6 from file: 350) **Links**
Derwent WPIX

009254901 **Image available**
WPI Acc No: 1992-382318/199246
XRPX Acc No: N92-291504

Fault tolerant network file system with primary and back-up servers - transfers data between file servers via dual ported memory and provides interrupt to receiving file server to notify change of data in memory

Patent Assignee: EASTMAN KODAK CO (EAST)
Inventor: MCGRATH J W; VINTHER G
Number of Countries: 015 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9218931	A1	19921029	WO 92US3001	A	19920414	199246	B
EP 536375	A1	19930414	EP 92909636	A	19920414	199315	

```
                              WO 92US3001     A   19920414
JP 5508506     W   19931125   JP 92509105     A   19920414  199401
                              WO 92US3001     A   19920414
```

Priority Applications (No Type Date): US 91690066 A 19910423
Cited Patents: 1.Jnl.Ref; EP 359471; US 4958270; WO 8909452
Patent Details:

```
Patent No  Kind Lan Pg   Main IPC    Filing Notes
WO 9218931    A1 E  43 G06F-011/20
   Designated States (National): JP
   Designated States (Regional): AT BE CH DE DK ES FR GB GR IT LU MC NL SE
EP 536375     A1 E     G06F-011/20   Based on patent WO 9218931
   Designated States (Regional): DE FR GB
JP 5508506    W        G06F-011/20   Based on patent WO 9218931
```

Abstract (Basic): WO 9218931 A

The system has primary (15) and **backup** (16) **file** servers connected to a dual ported memory (31). The **primary** file **server** writes data files to the memory and interrupts a processor (32) within the **backup file** server to notify it of new data. In response, the processor within the **backup file** server reads the data from the dual ported memoty and writes it to a storage device (34) within the **backup file** server. Data is also passed from the **backup** to **primary file servers**.

The dual ported memory includes semaphores for arbitrating between competing requests by the file servers for access to the same location.

USE/ADVANTAGE - In communications network links. Provides fault tolerant backup operation. High speed operation. Little computational cost. Transparent switching between file servers.

Dwg. 1/8

Title Terms: FAULT; TOLERATE; NETWORK; FILE; SYSTEM; PRIMARY; BACK-UP; SERVE; TRANSFER; DATA; FILE; SERVE; DUAL; PORT; MEMORY; INTERRUPT; RECEIVE; FILE; SERVE; NOTIFICATION; CHANGE; DATA; MEMORY
Derwent Class: T01; W01
International Patent Class (Main): G06F-011/20
International Patent Class (Additional): G06F-011/14; G06F-012/00
File Segment: EPI
Manual Codes (EPI/S-X): T01-F02; T01-F05; T01-G03; T01-J08C; W01-A06A1

?

[File 2] **INSPEC** 1898-2006/Jul W1
(c) 2006 Institution of Electrical Engineers. All rights reserved.

[File 6] **NTIS** 1964-2006/Jun W4
(c) 2006 NTIS, Intl Cpyrght All Rights Res. All rights reserved.

[File 8] **Ei Compendex(R)** 1970-2006/Jul W1
(c) 2006 Elsevier Eng. Info. Inc. All rights reserved.

[File 34] **SciSearch(R) Cited Ref Sci** 1990-2006/Jul W1
(c) 2006 Inst for Sci Info. All rights reserved.

[File 35] **Dissertation Abs Online** 1861-2006/Jun
(c) 2006 ProQuest Info&Learning. All rights reserved.

[File 65] **Inside Conferences** 1993-2006/Jul 10
(c) 2006 BLDSC all rts. reserv. All rights reserved.

[File 56] **Computer and Information Systems Abstracts** 1966-2006/Jun
(c) 2006 CSA. All rights reserved.

[File 57] **Electronics & Communications Abstracts** 1966-2006/Jun
(c) 2006 CSA. All rights reserved.

[File 60] **ANTE: Abstracts in New Tech & Engineer** 1966-2006/Jun
(c) 2006 CSA. All rights reserved.

[File 94] **JICST-EPlus** 1985-2006/Apr W2
(c)2006 Japan Science and Tech Corp(JST). All rights reserved.

[File 95] **TEME-Technology & Management** 1989-2006/Jul W2
(c) 2006 FIZ TECHNIK. All rights reserved.

[File 99] **Wilson Appl. Sci & Tech Abs** 1983-2006/Jun
(c) 2006 The HW Wilson Co. All rights reserved.

[File 111] **TGG Natl.Newspaper Index(SM)** 1979-2006/Jun 27
(c) 2006 The Gale Group. All rights reserved.

[File 144] **Pascal** 1973-2006/Jun W3
(c) 2006 INIST/CNRS. All rights reserved.

[File 266] **FEDRIP** 2005/Dec
Comp & dist by NTIS, Intl Copyright All Rights Res. All rights reserved.

[File 434] **SciSearch(R) Cited Ref Sci** 1974-1989/Dec
(c) 1998 Inst for Sci Info. All rights reserved.

[File 483] **Newspaper Abs Daily** 1986-2006/Jul 06

[File 583] **Gale Group Globalbase(TM)** 1986-2002/Dec 13

**File 583: This file is no longer updating as of 12-13-2002.*

```
 ; d s
Set     Items   Description
S1     302125   SERVER? OR RAS OR KEYSERVER? OR MAILSERVER? OR MULTISERVER? OR WEBSERVER?
OR PRINTSERVER? OR FILESERVER? OR HTTPSERVER? OR FTPSERVER? FROM 2, 6, 8, 34, 35, 65, 56,
57, 60, 94, 95, 99, 111, 144, 266, 434, 483, 583
S2        167   CLIENTSERVER? OR MICROSERVER? OR MINISERVER? OR PROXYSERVER? OR
DATASERVER? FROM 2, 6, 8, 34, 35, 65, 56, 57, 60, 94, 95, 99, 111, 144, 266, 434, 483, 583
S3          6   MAINSERVER? OR CENTRALSERVER? OR HEADSERVER? OR HOSTSERVER? OR LEADSERVER?
OR HEADSERVER? OR MASTERSERVER? OR CHIEFSERVER? FROM 2, 6, 8, 34, 35, 65, 56, 57, 60, 94,
95, 99, 111, 144, 266, 434, 483, 583
S4        443   ALPHASERVER? OR HUBSERVER? FROM 2, 6, 8, 34, 35, 65, 56, 57, 60, 94, 95,
99, 111, 144, 266, 434, 483, 583
S5       4111   (MAIN OR CENTRAL OR HEAD OR HOST OR LEAD OR MASTER OR CHIEF OR ALPHA OR
HUB OR CONTROL OR PRIMARY OR CENTER OR PARENT)(1W)S1:S2 FROM 2, 6, 8, 34, 35, 65, 56, 57,
60, 94, 95, 99, 111, 144, 266, 434, 483, 583
S6        611   (ADMINSTRAT???? ? OR PRINCIPAL OR PRINCIPLE OR LEADER OR CHIEF OR PRIME OR
ALPHA OR ARCHIV??? ? OR FOREMOST)(1W)S1:S2 FROM 2, 6, 8, 34, 35, 65, 56, 57, 60, 94, 95,
99, 111, 144, 266, 434, 483, 583
S7        162   (HEADMOST OR ORIGINAL OR HUB)(1W)S1:S2 FROM 2, 6, 8, 34, 35, 65, 56, 57,
60, 94, 95, 99, 111, 144, 266, 434, 483, 583
S8         12   SUPERIOR(1W)S1:S2 FROM 2, 6, 8, 34, 35, 65, 56, 57, 60, 94, 95, 99, 111,
144, 266, 434, 483, 583
S9        125   MAJOR(1W)S1:S2 FROM 2, 6, 8, 34, 35, 65, 56, 57, 60, 94, 95, 99, 111, 144,
266, 434, 483, 583
S10      1548   (SECONDARY OR LOCAL OR NODE OR CHILD OR SLAVE? OR BETA OR DEPENDENT OR
SUBORDINAT? OR INFERIOR OR MINOR OR SUBSERVIEN?)(1W)S1:S2 FROM 2, 6, 8, 34, 35, 65, 56,
57, 60, 94, 95, 99, 111, 144, 266, 434, 483, 583
S11        22   LOCALSERVER? OR NODESERVER? OR CHILDSERVER? OR SLAVESERVER? OR SUBSERVER?
OR BETASERVER? OR MINORSERVER? OR SUB()SERVER? FROM 2, 6, 8, 34, 35, 65, 56, 57, 60, 94,
95, 99, 111, 144, 266, 434, 483, 583
S12   1048908   DB OR DBS OR DATABASE? OR DATASET? OR DATABANK? OR DATASTORE? OR DATAFILE?
OR DATASYSTEM? OR DATALIBRAR? OR DATAMART? FROM 2, 6, 8, 34, 35, 65, 56, 57, 60, 94, 95,
99, 111, 144, 266, 434, 483, 583
S13    611357   DATA()(BASE? ? OR SET? ? OR BANK? ? OR STORE? ? OR FILE? ? OR SYSTEM? ? OR
LIBRAR??? ? OR MART? ? OR COLLECTION? OR DEPOSIT? OR REPOSIT?) FROM 2, 6, 8, 34, 35, 65,
56, 57, 60, 94, 95, 99, 111, 144, 266, 434, 483, 583
S14     14784   DATA()(WAREHOUS? OR STOREHOUS? OR (WARE OR STORE)()HOUS???? ?) FROM 2, 6,
8, 34, 35, 65, 56, 57, 60, 94, 95, 99, 111, 144, 266, 434, 483, 583
S15     30790   DBMS? OR RDB? ? OR VLDB? ? OR LDB? ? OR ODBC? ? OR OODB? ? OR RDBM? ? OR
OODM? ? OR ODBM? ? FROM 2, 6, 8, 34, 35, 65, 56, 57, 60, 94, 95, 99, 111, 144, 266, 434,
483, 583
S16    325787   FILE OR FILES FROM 2, 6, 8, 34, 35, 65, 56, 57, 60, 94, 95, 99, 111, 144,
266, 434, 483, 583
S17        41   COMPUTERFILE? OR TEXTFILE? FROM 2, 6, 8, 34, 35, 65, 56, 57, 60, 94, 95,
99, 111, 144, 266, 434, 483, 583
S18      2241   S12:S17(3N)(FREEZ? OR FROZE? OR LOCK??? ? OR LATCH? OR FLIPFLOP? OR
FLIP()FLOP? OR SUSPEND? OR SUSPENS? OR CEAS???? ? OR CESSATION?) FROM 2, 6, 8, 34, 35, 65,
56, 57, 60, 94, 95, 99, 111, 144, 266, 434, 483, 583
S19       450   S12:S17(3N)(INTERRUPT? OR ARREST? OR PAUS??? ? OR ABEYAN?) FROM 2, 6, 8,
34, 35, 65, 56, 57, 60, 94, 95, 99, 111, 144, 266, 434, 483, 583
```

```
S20         5   S12:S17(3N)TEMPORAR?(1W)(HALT??? ? OR STOP???? ? OR HOLD OR HELD OR
STAY??? ? OR DISCONTINU? OR INHIBIT?) FROM 2, 6, 8, 34, 35, 65, 56, 57, 60, 94, 95, 99,
111, 144, 266, 434, 483, 583
S21        12   S12:S17(3N)TEMPORAR?(1N)(HALT??? ? OR STOP???? ? OR HOLD OR HELD OR
STAY??? ? OR DISCONTINU? OR INHIBIT?) FROM 2, 6, 8, 34, 35, 65, 56, 57, 60, 94, 95, 99,
111, 144, 266, 434, 483, 583
S22     13129   S12:S17(3N)(REPLICA? OR DUPLICAT? OR COPIE? ? OR COPY??? ? OR MIRROR? OR
REPRODUC????? ? OR SHADOW? OR BACKUP? OR BACK??? ?()UP? ?) FROM 2, 6, 8, 34, 35, 65, 56,
57, 60, 94, 95, 99, 111, 144, 266, 434, 483, 583
S23      1119   S12:S17(3N)(CLONE? ? OR CLON??? ? OR FACSIMILE? OR RE()PRODUC????? ?) FROM
2, 6, 8, 34, 35, 65, 56, 57, 60, 94, 95, 99, 111, 144, 266, 434, 483, 583
S24        83   S S18:S21 AND S22:S23
S25         0   S S24 AND (S10:S11 OR S3:S9 OR CLIENTSERVER?)
S26        10   S S24 AND S1:S2
S27         1   S S26/2003:2006
S28         9   S S26 NOT S27
S29         5   RD  (unique items)

?  t 29/7/1,5
```

29/7/1 (Item 1 from file: 2) Links

INSPEC

08169043 **INSPEC Abstract Number:** C2002-03-6150N-011

Title: A data-centric concurrency control mechanism for three tier systems

Author Janaki Ram, D.; Chandra Sekhar, N.S.K.; Uma Mahesh, M.

Author Affiliation: Lab. for Distributed & Object Syst., Indian Inst. of Technol., Madras, India

Conference Title: 2001 IEEE International Conference on Systems, Man and Cybernetics. e-Systems and e-Man for Cybernetics in Cyberspace (Cat.No.01CH37236) **Part** vol.4 p. 2402-7 vol.4

Publisher: IEEE , Piscataway, NJ, USA

Publication Date: 2001 **Country of Publication:** USA 5 vol.3494 pp.

ISBN: 0 7803 7087 2 **Material Identity Number:** XX-2001-02743

U.S. Copyright Clearance Center Code: 0-7803-77-2/01/$10.00

Conference Title: Proceedings of IEEE International Conference on Systems, Man & Cybernetics

Conference Sponsor: Raytheon

Conference Date: 7-10 Oct. 2001 **Conference Location:** Tucson, AZ, USA

Language: English **Document Type:** Conference Paper (PA)

Treatment: Practical (P)

Abstract: Concurrency control (CC) algorithms targeted at Web systems need to be different from those of traditional transactional processing systems. In Web systems, transactions could be generated in a burst mode, leading to scalability problems at the **server**. Transactions may also suffer from network delays due to the unpredictable response time over the Web. This paper proposes a CC mechanism for Web-based three tier systems. In this mechanism, initial validation of the transactions is performed at the application **server**. The transactions that pass the initial validation are sent to the database **server** (**DB server**) for final validation. The serializability criterion is achieved by associating a data-counter with each data-item. This reduces the load on the DB **server**. Also, in the proposed model, the middle tier contains multiple number of application **servers**. Apart of the **database** is dynamically **replicated** in these **servers**. The modifications made on the data-items are known immediately to clients and the data-items at the **DB server** are **locked** only during the final validation phase and write phase. Consequently, the model is also suitable for transactions that suffer from unpredictable delays between read and write operations. The model is scalable as it can support large number of application **servers** in the middle tier. Performance studies have been carried out to depict the efficiency of the proposed model over the existing models.

The proposed model is simple to implement and it performs extremely well compared to existing models when the transactions are generated in a burst mode. (19 Refs)
Subfile: C

29/7/5 (Item 1 from file: 94) Links
JICST-EPlus

04324446 **JICST Accession Number:** 99A0909897 **File Segment:** JICST-E
An Investigation of the Way to Construct a Large-scale Distributed File System.
MIYAZAWA HAJIME (1) ; CHIBA SHIGERU (2)
(1) Nanzan Univ., Fac. of Manage. ; (2) Univ. of Tsukuba, Inst. of Inf. Sci. and Electron.
Denshi Joho Tsushin Gakkai Gijutsu Kenkyu Hokoku (IEIC Technical Report (Institute of Electronics, Information and Communication Enginners) , 1999 , VOL.99,NO.251(CPSY99 47-61) , PAGE.1-8 , FIG.4, TBL.2, REF.14
Journal Number: S0532BBG
Universal Decimal Classification: 681.3.066
Language: Japanese **Country of Publication:** Japan
Document Type: Journal
Article Type: Original paper
Media Type: Printed Publication
Abstract: We are developing the Aria large-scale distributed file system. Utilizing multiple **server** computers each of which has a whole **copy** of a **file** system, Aria realizes effective processing of access requests from many clients. Aria adopts the **interruption**/resumption of **files duplicated** among **server** computers to keep multiple **copies** of a **file** system consistent. Because the optimal algorithm that determines when to **interrupt**/resume **duplication** of **files** is unknown, we are investigating trace data of file accesses on file systems in real use to develop a better algorithm. This paper describes a preliminary investigation of file accesses on a file system in real use. (author abst.)

?

[File 9] **Business & Industry(R)** Jul/1994-2006/Jul 07
(c) 2006 The Gale Group. All rights reserved.

[File 16] **Gale Group PROMT(R)** 1990-2006/Jul 07
(c) 2006 The Gale Group. All rights reserved.

[File 47] **Gale Group Magazine DB(TM)** 1959-2006/Jul 06
(c) 2006 The Gale group. All rights reserved.

[File 148] **Gale Group Trade & Industry DB** 1976-2006/Jul 06
(c)2006 The Gale Group. All rights reserved.

[File 160] **Gale Group PROMT(R)** 1972-1989
(c) 1999 The Gale Group. All rights reserved.

[File 275] **Gale Group Computer DB(TM)** 1983-2006/Jul 07
(c) 2006 The Gale Group. All rights reserved.

[File 621] **Gale Group New Prod.Annou.(R)** 1985-2006/Jul 06
(c) 2006 The Gale Group. All rights reserved.

[File 624] **McGraw-Hill Publications** 1985-2006/Jul 07
(c) 2006 McGraw-Hill Co. Inc. All rights reserved.
**File 624: Homeland Security & Defense and 9 Platt energy journals added Please see HELP NEWS624 for more*

[File 634] **San Jose Mercury** Jun 1985-2006/Jul 07
(c) 2006 San Jose Mercury News. All rights reserved.

[File 649] **Gale Group Newswire ASAP(TM)** 2006/Jun 27
(c) 2006 The Gale Group. All rights reserved.

[File 636] **Gale Group Newsletter DB(TM)** 1987-2006/Jul 07
(c) 2006 The Gale Group. All rights reserved.

[File 647] **CMP Computer Fulltext** 1988-2006/Aug W2
(c) 2006 CMP Media, LLC. All rights reserved.

[File 674] **Computer News Fulltext** 1989-2006/Jun W3
(c) 2006 IDG Communications. All rights reserved.

```
 ; d s
Set      Items   Description
S1     2054172   SERVER? OR RAS OR KEYSERVER? OR MAILSERVER? OR MULTISERVER? OR WEBSERVER?
OR PRINTSERVER? OR FILESERVER? OR HTTPSERVER? OR FTPSERVER? FROM 9, 16, 47, 148, 160, 275,
621, 624, 634, 649, 636, 647, 674
S2        3349   CLIENTSERVER? OR MICROSERVER? OR MINISERVER? OR PROXYSERVER? OR
DATASERVER? FROM 9, 16, 47, 148, 160, 275, 621, 624, 634, 649, 636, 647, 674
S3          52   MAINSERVER? OR CENTRALSERVER? OR HEADSERVER? OR HOSTSERVER? OR LEADSERVER?
```

```
OR HEADSERVER? OR MASTERSERVER? OR CHIEFSERVER? FROM 9, 16, 47, 148, 160, 275, 621, 624,
634, 649, 636, 647, 674
S4       7471   ALPHASERVER? OR HUBSERVER? FROM 9, 16, 47, 148, 160, 275, 621, 624, 634,
649, 636, 647, 674
S5      54003   (MAIN OR CENTRAL OR HEAD OR HOST OR LEAD OR MASTER OR CHIEF OR ALPHA OR
HUB OR CONTROL OR PRIMARY OR CENTER OR PARENT)(1W)S1:S2 FROM 9, 16, 47, 148, 160, 275,
621, 624, 634, 649, 636, 647, 674
S6       8727   (ADMINSTRAT???? ? OR PRINCIPAL OR PRINCIPLE OR LEADER OR CHIEF OR PRIME OR
ALPHA OR ARCHIV??? ? OR FOREMOST)(1W)S1:S2 FROM 9, 16, 47, 148, 160, 275, 621, 624, 634,
649, 636, 647, 674
S7       1890   (HEADMOST OR ORIGINAL OR HUB)(1W)S1:S2 FROM 9, 16, 47, 148, 160, 275, 621,
624, 634, 649, 636, 647, 674
S8        776   SUPERIOR(1W)S1:S2 FROM 9, 16, 47, 148, 160, 275, 621, 624, 634, 649, 636,
647, 674
S9       5684   MAJOR(1W)S1:S2 FROM 9, 16, 47, 148, 160, 275, 621, 624, 634, 649, 636,
647, 674
S10     12347   (SECONDARY OR LOCAL OR NODE OR CHILD OR SLAVE? OR BETA OR DEPENDENT OR
SUBORDINAT? OR INFERIOR OR MINOR OR SUBSERVIEN?)(1W)S1:S2 FROM 9, 16, 47, 148, 160, 275,
621, 624, 634, 649, 636, 647, 674
S11        71   LOCALSERVER? OR NODESERVER? OR CHILDSERVER? OR SLAVESERVER? OR SUBSERVER?
OR BETASERVER? OR MINORSERVER? OR SUB()SERVER? FROM 9, 16, 47, 148, 160, 275, 621, 624,
634, 649, 636, 647, 674
S12   2307200   DB OR DBS OR DATABASE? OR DATASET? OR DATABANK? OR DATASTORE? OR DATAFILE?
OR DATASYSTEM? OR DATALIBRAR? OR DATAMART? FROM 9, 16, 47, 148, 160, 275, 621, 624, 634,
649, 636, 647, 674
S13    687473   DATA()(BASE? ? OR SET? ? OR BANK? ? OR STORE? ? OR FILE? ? OR SYSTEM? ? OR
LIBRAR??? ? OR MART? ? OR COLLECTION? OR DEPOSIT? OR REPOSIT?) FROM 9, 16, 47, 148, 160,
275, 621, 624, 634, 649, 636, 647, 674
S14    138252   DATA()(WAREHOUS? OR STOREHOUS? OR (WARE OR STORE)()HOUS???? ?) FROM 9, 16,
47, 148, 160, 275, 621, 624, 634, 649, 636, 647, 674
S15    130353   DBMS? OR RDB? ? OR VLDB? ? OR LDB? ? OR ODBC? ? OR OODB? ? OR RDBM? ? OR
OODM? ? OR ODBM? ? FROM 9, 16, 47, 148, 160, 275, 621, 624, 634, 649, 636, 647, 674
S16   2130108   FILE OR FILES FROM 9, 16, 47, 148, 160, 275, 621, 624, 634, 649, 636, 647,
674
S17       196   COMPUTERFILE? OR TEXTFILE? FROM 9, 16, 47, 148, 160, 275, 621, 624, 634,
649, 636, 647, 674
S18     13979   S12:S17(3N)(FREEZ? OR FROZE? OR LOCK??? ? OR LATCH? OR FLIPFLOP? OR
FLIP()FLOP? OR SUSPEND? OR SUSPENS? OR CEAS???? ? OR CESSATION?) FROM 9, 16, 47, 148, 160,
275, 621, 624, 634, 649, 636, 647, 674
S19      2443   S12:S17(3N)(INTERRUPT? OR ARREST? OR PAUS??? ? OR ABEYAN?) FROM 9, 16, 47,
148, 160, 275, 621, 624, 634, 649, 636, 647, 674
S20        30   S12:S17(3N)TEMPORAR?(1W)(HALT??? ? OR STOP???? ? OR HOLD OR HELD OR
STAY??? ? OR DISCONTINU? OR INHIBIT?) FROM 9, 16, 47, 148, 160, 275, 621, 624, 634, 649,
636, 647, 674
S21       118   S12:S17(3N)TEMPORAR?(1N)(HALT??? ? OR STOP???? ? OR HOLD OR HELD OR
STAY??? ? OR DISCONTINU? OR INHIBIT?) FROM 9, 16, 47, 148, 160, 275, 621, 624, 634, 649,
636, 647, 674
S22    107399   S12:S17(3N)(REPLICA? OR DUPLICAT? OR COPIE? ? OR COPY??? ? OR MIRROR? OR
REPRODUC????? ? OR SHADOW? OR BACKUP? OR BACK??? ?()UP? ?) FROM 9, 16, 47, 148, 160, 275,
621, 624, 634, 649, 636, 647, 674
S23      2159   S12:S17(3N)(CLONE? ? OR CLON??? ? OR FACSIMILE? OR RE()PRODUC????? ?) FROM
9, 16, 47, 148, 160, 275, 621, 624, 634, 649, 636, 647, 674
S24       779   S S18:S21(S)S22:S23
S25         9   S S24(S)(S10:S11 OR S3:S9 OR CLIENTSERVER?)
S26       215   S S24(S)S1:S2
S27         3   S S25/2003:2006
S28         6   S S25 NOT S27
S29         6   RD  (unique items)
 ; t 29/3,k/5-6
```

29/3,K/5 (Item 1 from file: 674) **Links**

Computer News Fulltext

045331

Forgiving NETWORK FAULTS

NetworkWorld Review, NetworkWorld TEST ALLIANCE

Constantly worrying because your network has to be up around the clock? These four products make it easier for you to relax.

Byline: Howard Marks
Journal: Network World **Page Number:** 31
Publication Date: July 03, 1995
Word Count: 2488 **Line Count:** 222
Text:

...for these nets. The products we tested help keep downtime to a minimum by saving **copies** of crucial **files**. Each uses different mechanisms to meet the requirements of high-availability computing, but all improve network reliability. Horizons Technology, Inc.'s LANshadow uses a periodic **copy** function to protect **files**, making it suitable for organizations such as law firms, whose work involves a multiplicity of ...

...perform maintenance. You can similarly break the link between the servers and back up the **secondary server** to tape while users continue to access the **primary server**. When using any of these server-based systems, you must be careful to periodically test to make sure the **secondary server** can support all your applications at the same time. We've seen network administrators configure systems that didn't work in an emergency because the **primary server** had its disk, memory and NetWare Loadable Module (NLM) configuration upgraded while the backup server...

...its modest beginnings as a DOS application that ran on a dedicated personal computer to **copy files** from one server to another. LANshadow now uses an NLM but is still more an...

...system than a true provider of fault tolerance. LANshadow allows a network administrator to automatically **copy files** from one NetWare 3.X or 4.X file server to another. The LANshadow NLM on the destination file server logs on to the source **file** server and **copies files** from the designated directories that have changed since the last cycle. The network administrator can...

...source/destination directory pairs. A single-source directory can have multiple destinations, and a single **file** server can **back up** multiple servers. Administrators can exclude **files** from the **backup** process and can even designate a group of files to be a file family that must be copied together. When LANshadow **copies** a **file** family, it **locks** all the **files** in the family before copying them to ensure that they are all in sync with one another. LANshadow Version 4.0 adds the ability to **copy** Macintosh **files** and to establish what Horizons calls no-**lock**

file families, which can be backed up even if other users have these files open. LANshadow...

...pair can have an individual schedule that overrides the master for that pair. LANshadow can **copy files** at up to 15M byte/min and scan files to see if they need to...

...user makes an update to a 1G-byte database, it will be hours before that **database** is completely **backed up**. This makes LANshadow a better solution for protecting word processing and other small files that ...

...disk drives over the SCSI bus as if the switch wasn't there. If the **primary server** fails, you just flip the switch to connect the disks to the backup server and boot the **backup** as your **file** server. NetGuard has taken this concept to its ultimate level by also connecting a serial...

...from each of the two file servers to the switch and adding NLMs to the **primary** file **server** that talk to a DOS program on the backup. Should the backup server fail to communicate with the **primary server**, it uses its second serial connection to the NSI 5000-100 to flip the switch...systems status. Like StandbyServer 32, NetGuard's software addresses the fact that the primary and **secondary servers** might have different hardware configurations by storing additional AUTOEXEC. NCF information in a **backup** server **file** and swapping the files as part of the reboot process. In our testing, the NSI...
...you to build a system that uses one standby server to protect data on several **primary servers** through multiple SCSI switches. Of course, the standby server can only replace one server at...

...a more cost-effective solution than having a dedicated standby server for each of several **primary servers**. NonStops NoStop Network Unlike the other products reviewed, NoStop Network takes a workstation approach to...

...to the secondary member of the pair. To ensure data integrity, No-Stop Network also **duplicates file** and record **lock** requests so that **databases** on the secondary drive are protected. The secondary member of the pair, therefore, has an...

...duplicates requests for users of the Btrieve Virtual Loadable Module (VLM) database server, so Btrieve **databases** can be **mirrored** to **duplicate database** servers. If a read error is reported on a primary drive, NoStop Network traps the...

...pair to be on separate file servers, users can continue to work even if the **primary server** fails. Unlike with Novell, Inc.'s System Fault Tolerance III (SFT III), the two servers...would have to manually restart the standby ser-ver as a NetWare server when the **primary server** failed. With Vinca's new Autoswitch option, if the standby server can't communicate with the **primary server** over either the server-to-server link or over the LAN via IPX, it automatically restarts itself as the failed **primary** NetWare **server** after a short countdown. The Autoswitch process automatically updates the AUTOEXEC.NCF and STARTUP.NCF...

...s Vrepair utility if the volumes on the mirrored drive are damaged due to the **primary server** failure. After disk volumes are repaired, they are automatically mounted. In our testing, running StandbyServer...

...pair of drives from a single host adapter. When we pulled the plug on the **primary server**, the backup was up within 5 minutes. For users running Version 1.20 of Novell's VLM, which automatically reconnects to servers, a **primary server** failure looks like a momentary interruption. Different strokes For many net administrators, NoStop Network is...

29/3,K/6 (Item 2 from file: 674) Links
Computer News Fulltext

045010

Vinca takes LANs a step forward with on-line backup capability

Byline: Margaret Dornbusch
Journal: Network World **Page Number:** 1
Publication Date: June 19, 1995
Word Count: 472 **Line Count:** 43
Text:

Orem, Utah Software that provides on-line **backup** of **databases** and open files in a LAN environment will be revealed this week by Vinca Corp. Designed to work in conjunction with Vinca's StandbyServer product, which mirrors data from a **primary server** to a **secondary server**, SnapShot Server gives net managers the ability to perform backups without having to take the server down. SnapShot Server, which runs on the **secondary server**, takes a snapshot of the files coming into the **secondary server** and places that data into a temporary, virtual hard drive. The information in that drive...

...popular backup program, said Greg Brashier, Vinca's vice president of marketing. The software can **back up** databases and open **files** without **interrupting** or slowing the **primary server** since it uses data already being mirrored to the **secondary server**, Brashier said. SnapShot Server used in conjunction with StandbyServer provides net managers with outstanding protection...

...to using SnapShot Server is that if something goes wrong with the backup

process, the **main server** is not affected since backup
software runs on the **secondary server**, Brashier said. Also,
the backup runs much quicker since, aside from the mirroring application,
there is nothing running on the **secondary server**. SnapShot
Server currently runs only on NetWare 4.X networks, but a version for Vinca
...

?